



UNITED STATES MARINE CORPS

III MARINE EXPEDITIONARY FORCE, FMF

UNIT 35601

FPO AP 96606-5601

ForO P2281.2

6

19 AUG 1994

FORCE ORDER P2281.2

From: Commanding General
To: Distribution List

Subj: III MARINE EXPEDITIONARY FORCE COMMUNICATION SECURITY
MANAGEMENT OFFICE (MCMO) INTERNAL OPERATING PROCEDURES
(SHORT TITLE: MCMO IOP)

Ref: (a) CMS 1
(b) CMC WASHINGTON DC 041900Z Jan 93
(c) ForO 2281.1
(d) ForO 5510.16A

Encl: (1) LOCATOR SHEET

1. Purpose. To promulgate the policies, procedures, and standards for the effective management, operation and maintenance of the MCMO per reference (a) and this Manual.


2. Background. Reference (b) directed the establishment of COMSEC Management Offices at each MEF to accomplish the following objectives.

a. Place Communication Security Material System (CMS) accountability/control into the operational chain of command vice separate accounts.

b. Reduce the quantity of Communication Security (COMSEC) keying material held at the unit level and improve operational readiness by ensuring required keying material availability.

3. Recommendations concerning the contents of the MCMO IOP are invited. Such recommendations will be forwarded to the III MEF AC/S, G-6 via the appropriate chain of command.

4. Certification. Reviewed and approved this date.


J. L. BRENNAN
Chief of Staff

DISTRIBUTION: LIST I 2,6

ForO P2281.2
19 AUG 1994

LOCATOR SHEET

Subj: III MEF COMMUNICATIONS SECURITY MANAGEMENT OFFICE INTERNAL
OPERATION PROCEDURES

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

ENCLOSURE (1)

MCMO IOP

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

MCMO IOP

CONTENTS

CHAPTER

- 1 PERSONNEL, RESPONSIBILITIES AND DUTIES
- 2 VAULT SECURITY
- 3 PROCOESSING OF MESSAGE TRAFFIC AND MAINTENANCE OF CMS FILES
- 4 INCOMING MATERIAL PROCESSING PROCEDURES
- 5 DISTRIBUTION PROCEDURES
- 6 PROCEDURES FOR PREPARING CMS MATERIAL FOR SHIPMENT
- 7 CMS EMERGENCY ISSUE PROCEDURES
- 8 DESTRUCTION PROCEDURES

MCMO IOP

CHAPTER 1

PERSONNEL, RESPONSIBILITIES AND DUTIES

	<u>PARAGRAPH</u>	<u>PAGE</u>
DUTIES, RESPONSIBILITIES AND QUALIFICATIONS..	1000	1-3
MEF COMSEC MANAGEMENT OFFICER.....	1001	1-3
MCMO CHIEF.....	1002	1-4
DISTRIBUTION AND ALLOWANCE (D&A) CHIEF.....	1003	1-5
VAULT OPERATIONS CHIEF.....	1004	1-6
ADMINISTRATIVE CHIEF.....	1005	1-7
CMS CLERKS.....	1006	1-7

MCMO IOP

CHAPTER 1

PERSONNEL, RESPONSIBILITIES AND DUTIES

1000. DUTIES, RESPONSIBILITIES AND QUALIFICATIONS. Specific billets are assigned within the MCMO, CMS Custodians will become familiar with every aspect of the office. Custodians can expect to be rotated amongst the D&A, Vault Operations and Administrative Chief billets. Additionally, custodians will be expected to respond to STU-III trouble calls, execute Over-the-Air Distribution (OTAD) procedures, perform CMS courier duties and serve as CMS Inspectors. Besides the CMS Custodian designation requirements outlined in reference (a), the MCMO requires its custodians at least 9 months time remaining on station before designated a MCMO Custodian.

1001. MEF COMSEC MANAGEMENT OFFICER (MCMO OFFICER). The MCMO Officer is responsible to the III MEF Staff CMS Responsibility Officer (AC/S, G-6) for the efficient operation and accountability of all CMS material received/distributed by the MCMO. Specifically, the duties include the following.

1. Establish, supervise and execute COMSEC policies, procedures and administrative requirements for the MCMO.
2. Serve as an alternate custodian for the MCMO; perform security checks on incoming/outgoing CMS material; identify/reconcile discrepancies; initiate discrepancy reports; conduct periodic inventories to ensure proper accountability; and maintain safe combinations as necessary for Two Person Integrity (TPI).
3. Serve as the III MEF COMSEC Employment Officer; publish COMSEC "Call-Outs" and COMSEC appendices to the annex K of III MEF Operation Orders.
4. Serve as the Controlling Authority for III MEF key systems and perform duties per reference (a).
5. Serve as III MEF Item Manager for cryptographic hardware. Coordinate with subordinate command CMS Custodians and the III MEF Supply Officer to ensure that required/authorized cryptographic hardware is on-hand and properly reported in both COMSEC Material and Supply Systems.

6. As required, recommend reallocation of COMSEC assets among subordinate commands to ensure maximum benefit of available assets are achieved.

7. Serve as the Command Authority for the III MEF STU-III accounts.

1002. MCMO CHIEF. The MCMO Chief is the account's primary custodian and responsible to the MCMO Officer for monitoring account operations and performing the duties of the officer in charge in his absence. The MCMO Chief reports to the MCMO Officer on all matters concerning MCMO operations. The following are specific responsibilities.

1. As the primary custodian for the MCMO account, supervise its daily operations per references (a), (c) and this Manual.

2. Perform security checks on incoming/outgoing CMS material; identify and reconcile discrepancies; initiate discrepancy reports; verify material scheduled for destruction and transfer; prepare destruction reports; conduct periodic inventories to ensure proper accountability; and maintain safe combinations as required for TPI.

3. Ensure courteous, efficient service and provide information to Unit CMS Custodian's on allowances, distribution, accounting, security, deployment and other account management issues.

4. Ensure personnel are familiar with the instructions and security requirements pertinent to handling COMSEC material and that individuals are properly supervised and trained in MCMO duties.

5. Provide technical advice and assistance to the COMSEC Management Officer, MCMO Custodians, Commanding Officers and other command representatives.

6. Publish "Effective Status" messages for all III MEF Controlled COMSEC Material.

7. Evaluate cryptographic/physical insecurities and recommend corrective actions.

8. Serve as the Senior Inspector on MCMO Inspection Teams.

9. Supervise the proper management of the III MEF STU-III account.

1003. D&A CHIEF. The D&A Chief is an alternate custodian and responsible for distribution and allowance operations. The D&A Chief reports to the MCMO Chief on all technical, administrative and operational matters. The following are specific responsibilities.

1. Ensure contingency Automated Distribution Procedures are current and executed (for training purposes) on a quarterly basis.
2. Maintain Unit Allowance Cards for the Commander in Chief, Pacific (CINCPAC) and Central Command (CENTCOM) Area of Responsibility.
3. Maintain a current file on all III MEF Defense Courier Service (DCS) addresses and deployment schedules.
4. Review all COMSEC "Call-Outs" to ensure III MEF commands and units attached to III MEF have required/sufficient keying material.
5. Coordinate all COMSEC issues and shipments with Unit Custodians and the Vault Operations Chief.
6. Coordinate the establishment and logistic support of III MEF controlled keying material by advising COMSEC Material Issuing Office (CMIO), San Diego and National Security Agency (NSA) Y13 of the COMSEC accounts that are to receive keying material and number of copies.
7. In coordination with the Vault Operations Chief, adjust the Automated COMSEC Reporting System (ANCRS) database to reflect changes requested by CMS account holders and authorized by Director, Communications Security Material System (DCMS) and Controlling Authorities.
8. Coordinate all routine modification of allowances for keying material.
9. Submit "Effective Status" messages on all III MEF keying material to the MCMO Chief.
10. Annually contact III MEF keying material holders to identify the keying material they control and a III MEF point of contact.

11. Review all stock levels to identify superseded editions, and deficient or excessive quantities.

12. Issue all CMS material, maintain CMS "SKINNY SHEETS" and coordinate with the Vault Operations Chief on assignment of Transaction Numbers for material issues.

1004. VAULT OPERATIONS CHIEF. The Vault Operations Chief serves as an alternate custodian and is responsible for the physical security and accountability of the MCMO account. The Vault Operations Chief reports to the MCMO Chief on all technical, administrative and operational matters. The following are specific responsibilities.

1. Coordinate all physical security measures per reference (a), specifically the following:

a. Ensure combination changes and assignments have been coordinated for the vault and its security containers.

b. Coordinate all facility upgrades.

c. Ensure proper Opening/Closing procedures are maintained.

d. Maintain MCMO Visitor's Log.

e. Maintain copies of SF 701 (Security Container Checklist) and SF 702 (Security Container Check Sheet).

f. Conduct Emergency Action Procedure training per reference (a).

2. Receive, store, safeguard, distribute, destroy, report and account for all CMS material held by the MCMO.

3. Review daily message traffic for items effecting vault operations and initiate required actions.

4. Coordinate deliveries with the Defense Courier Service.

5. Supervise Destruction "Double Check" and "Final Check" Teams.

6. Report all transaction into the ANCRS System.

7. Per reference (a), maintain Chronological Files, Transaction Logs, and COMSEC Material Accounting Reports and Local Custody Files.

8. Conduct Fixed Cycle, Special, Combined or Miscellaneous Inventories per reference (a).
9. Assist the D&A Chief in preparing over-the-counter issues and deliveries during Emergency Issues.

1005. ADMINISTRATIVE CHIEF. The Administrative Chief is responsible for managing the MCMOs numerous administrative requirements, STU-III account and performing Alternate Custodian duties. The Administrative Chief reports to the MCMO Chief on all technical, administrative and operational matters. The following are specific responsibilities.

1. Per reference (a), maintain CMS Correspondence and Message, General Message, Directives Files and CMS Publications Library and accountability of all items subsigned from the CMCC.
2. Review, segregate, maintain and reproduce incoming/outgoing correspondence.
3. Review Standard Subject Identification Codes (SSIC) and General Message files annually. Destroy messages which are more than 2 years old or cancelled.
4. Maintain list of Address Indicator Groups that III MEF MCMO is an addressee.
5. Coordinate all MCMO sponsored training evolutions and inspections.
6. Maintain and promulgate schedules and weekly events calendars.
7. Maintain MCMO Self-Service Items and budget history.
8. Ensure MCMO Recall Roster and Emergency Recall Instructions are current in the III MEF Command Center.

1006. CMS CLERKS. Clerks may assist with CMS material receipt, issue, inventory, destruction etc., and may also be used to maintain two-person integrity protection of material once security containers are opened. CMS Clerks are not alternate custodians and will not perform CMS custodial duties in place of an alternate custodian.

MCMO IOP

CHAPTER 2

VAULT SECURITY

	<u>PARAGRAPH</u>	<u>PAGE</u>
TWO PERSON INTEGRITY (TPI) VAULT.....	2000	2-3
OPENING PROCEDURES.....	2001	2-3
CLOSING PROCEDURES.....	2002	2-4
VISITORS.....	2003	2-4
ACCESS TO AND PROTECTION OF SAFE COMBINATIONS..	2004	2-4
EMERGENCY ACTION PROCEDURES (EAP).....	2005	2-4
MCMO AND SECURITY MANAGER RELATIONSHIP.....	2006	2-4

MCMO IOP

CHAPTER 2

VAULT SECURITY

2000. TWO PERSON INTEGRITY (TPI) VAULT

1. Per reference (a), TPI handling requires that at least two persons, authorized access to COMSEC keying material, be in constant view of each other and the COMSEC material requiring TPI whenever that material is accessed and handled. Each individual must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

2. The CMS Vault in Bldg 4225, Room 125, Camp Courtney is a TPI Open Storage Vault for SECRET and below materials marked CRYPTO and requires extraordinary security safeguards based on the following principles.

a. No one person will have access to both combinations to the CMS Vault, nor the TOP SECRET security containers inside the vault.

b. While the CMS Vault is open it is considered a "NO LONE ZONE." Two Marines from the MCMO "Authorized Access" list will always be present in the CMS Vault while it remains "OPEN." Additionally, one of these individuals must be a designated custodian from the MCMO account. Violation to these principles will not be tolerated and will be grounds for disciplinary action.

2001. OPENING PROCEDURES. Given that the MCMO facility is a TPI Vault at least one custodian must be present to open/close the CMS Vault. The following procedures apply.

1. Prior to opening the front lock, MCMO personnel will conduct a external security inspection of the vault to ensure there is no sign of forced entry. This inspection will include the door jambs, locks and knobs. Any sign of forced entry will immediately be reported to the III MEF Command Duty Officer (CDO). Personnel will not enter the MCMO if evidence of forced entry exists.

2. Upon opening the second lock, both individuals involved in opening the TPI locks must initial the SF-702 (Security Container Checklist). Additionally, the two Marines will sign in on the TPI Logbook with Name/Time-in/Time-out.

3. At this time the CMS Vault is considered a "NO LONE ZONE" and TPI principles apply. If an individual must leave the vault, their TPI replacement must record their Name/Time-in/Time-out in the TPI Log Book to verify TPI is being maintained.

2002. CLOSING PROCEDURES

1. Approximately 15 minutes prior to the end of the working day, MCMO personnel will return classified material to the security of the TPI Vault and TOP SECRET safes.

2. A MCMO TPI Team tasked with closing, will initial actions completed on the Daily Security Checkout Log and the SF-702 (Security Container Checklist).

3. If a security problem cannot be corrected, the MCMO Custodian will contact the CDO and remain in the facility until the situation is resolved. Overnight watches will be established until the situation can be corrected.

2003. VISITORS. A visitor is defined as a person not assigned to the MCMO for duty. Visitors will be logged into the Visitor's Log and escorted at the front hatch prior to entry. Visitors will be escorted at all times while in the TPI Vault. All personal articles brought into the MCMO Vault are susceptible to search at any time. No person will remove CMS material or classified non-CMS material from the MCMO vault except in the official performance of their duties.

2004. ACCESS TO AND PROTECTION OF SAFE COMBINATIONS. Procedures outlined in reference (d) will be followed. A copy of all Vault and container combinations will be sealed and secured in the III MEF Command Center.

2005. EMERGENCY ACTION PROCEDURES (EAP). These procedures are posted on the front of the vault with the sealed combinations in the Command Center. EAP are per reference (a).

2006. MCMO AND SECURITY MANAGER RELATIONSHIP. The Security Manager's realm of responsibility is limited to matters and material which are routine security management procedures and shall not detract from the CMS Custodian's authority for CMS related security matters. The Security Manager is responsible for ensuring appropriate physical security inspections and surveys are conducted, security clearances and special access authorizations

2002

MCMO IOP

(other than CMS) are updated and accurate, handling/storage of classified material other than COMSEC material are per the DON Security Program, and for conducting initial investigations of possible insecurities/COMSEC incidents.

MCMO IOP

CHAPTER 3

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	3000	3-3
PROCESSING INCOMING CLASSIFIED MESSAGES.....	3001	3-3
PROCESSING INCOMING UNCLASSIFIED MESSAGES.....	3002	3-3
PROCESSING OUTGOING CLASSIFIED MESSAGES.....	3003	3-4
PROCESSING OUTGOING UNCLASSIFIED MESSAGES.....	3004	3-4
CMS FILES.....	3005	3-4

MCMO IOP

CHAPTER 3

PROCESSING OF MESSAGE TRAFFIC AND MAINTENANCE OF CMS FILES

3000. GENERAL. MCMO personnel are responsible for reviewing and safeguarding message traffic. CMS GENERAL MESSAGE FILES will be maintained electronically via Message Dissemination SubSystem (MDS) and downloaded to a designated directory in the Local Management Device (LMD) C:\ drive. This directory will be "backed-up" daily on diskette and a GENERAL MESSAGE FILE LOG will be kept recording the classification/DTG/Originator/Subj. Hard copy message traffic will be produced as required.

3001. PROCESSING INCOMING CLASSIFIED MESSAGES. The Administrative Chief will maintain a "CLASSIFIED" diskette, color-coded "red" and marked SECRET, to download files into the "General Message" file directory located in the LMD.

Step 1. Each day the CMS Clerk will receive a "CLASSIFIED" diskette from the CLASSIFIED MDS Workstation and ensure the number recorded on the diskette matches the numbered diskette returned the afternoon prior. The CMS Clerk will download the files into the "General Message" file directory located in the LMDs C:\ drive.

Step 2. The Administrative Chief tags messages and places tasking notes on those messages that require "ACTION." The electronic "Read Board" will then be available to the remainder of MCMO personnel.

Step 3. Following review by the MCMO staff, the CMS Clerk will record messages to be downloaded into the "General Message" File LOG in Classification/Date-Time-Group/Originator/Subject format. The CMS Clerk will then download the "tagged" files into the "General Message" file directory and back-up diskette.

Step 4. Once the download is complete, the CMS Clerk will delete the files from the diskette, record the CLASSIFIED diskette number into the "General Message" file Log and return the diskette to the CLASSIFIED MDS Workstation.

3002. PROCESSING INCOMING UNCLASSIFIED MESSAGES. The Administrative Chief will access the MCMO MDS account via the III MEF Local Area Network. Files will be recorded in the GENERAL MESSAGE FILES LOG and downloaded into the designated directory in the LMDs C:\ drive. The MDS account will not be deleted until all MCMO personnel have reviewed the electronic "Read Board."

3003. PROCESSING OUTGOING CLASSIFIED MESSAGES

Step 1. Classified message traffic will be composed using the MTF Editor Program on the LMD Workstation and stored on a diskette marked "CONFIDENTIAL."

Step 2. The classified message will be proofread by the Administrative Chief, error checked via MTF, scanned by the Distributed Plain Language Verification Address System (DPVS) and logged into the "OUTGOING MESSAGE TRAFFIC" Log.

Step 3. A hard copy and diskette will be submitted to the COMSEC Management Officer for review, who in turn submits the message to the III MEF Communications Chief for release. Upon signature by the AC/S, G-6, the message will be released and diskette returned.

3004. PROCESSING OUTGOING UNCLASSIFIED MESSAGES

Step 1. Unclassified messages will be composed using the MTF Editor Program on the Local Area Networks S:\ drive.

Step 2. The message will be attached to an E-mail and sent to the Administrative Chief for proofreading and recording. The Administrative Chief will then send (via the S:\ drive) the message to the III MEF Communications Chief for release.

3005. CMS FILES. The following CMS files will be maintained by the designated billet holder per reference (a) and this Manual.

<u>BILLET</u>	<u>CMS FILE</u>
Administrative Chief	General Message File Correspondence and Message File Directives File CMS Publications Library
Vault Operations Chief	CMS Chronological File Local Custody File
D&A Chief	Unit Allowance Cards "SKINNY SHEETS" DCS Address List Deployment/UDP Schedules Exercise COMSEC Call-Outs ICP Files CINCPAC Files III MEF Controlling Authority Files

MCMO IOP

CHAPTER 4

INCOMING MATERIAL PROCESSING PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	4000	4-3
CMIO SHIPMENTS: MATERIAL RECEIPT AND PROCESSING PROCEDURES.....	4001	4-3
UNIT CUSTODIAN TURN-IN OF EXCESS MATERIAL.....	4002	4-4

MCMO IOP

CHAPTER 4

INCOMING MATERIAL PROCESSING PROCEDURES

4000. GENERAL. A MCMO Custodian and CMS Ckerj will verify and receipt for all incoming material. MCMO personnel will assist with off-loading and storing the material in the TPI Vault. Shipments will be offloaded in the rear of BLDG 4225.

4001. CMIO SHIPMENTS: MATERIAL RECEIPT AND PROCESSING PROCEDURES. The following procedures apply for material received from CMIO via the DCS.

STEP 1. The D&A Chief will receipt for the material from DCS, verify that there are no discrepancies in the MCMO DCS address and retrieve both the SF-153 (normally found in container #1) and DCS Form 32.

WARNING: MCMO personnel will wear gloves, long sleeves and face shields/goggles when cutting the banding off large CMIO shipments. The banding will be placed in the "BANDING BOX" for disposal. At no time will banding be placed in the garbage containers within the MCMO.

STEP 2. If the SF-153 does not indicate the DCS number assigned to that particular shipment, the D&A Chief will record the DCS number on the top left of the SF-153 and mark the discrepancy on the DCS Form 32 accompanying the shipment. Form 32 will be forwarded to the Vault Operations Chief to place in the Chronological File for future action.

STEP 3. Open containers in sequential order (indicated on the DCS Form 32) and place material on the working counter in the same order indicated on the respective SF-153. Flatten DCS boxes and store them in designated areas away from the working counter.

NOTE: Material received in more than one container may have the series indicated on each container (i.e., 1/3, 2/3, 3/3). If not, DCS numbers, as listed on the Form 32, should be in sequential order allowing identification of container #1.

STEP 4. Verify that material received is not superseded per the CSPM-3 and effective status messages. If the material is

superseded, place the material on the "AWAITING DISPOSITION" shelf. The Vault Ops Chf will prepare a "DESTRUCTION" SF-153 and destroy superseded material per ref (a).

STEP 5. The D&A Chief updates his Unit Allowance Cards, initials the SF-153 and returns it to the Vault Ops Chf for storage and further processing per reference (a).

4002. UNIT CUSTODIAN TURN-IN OF EXCESS MATERIAL. The following procedures apply for Unit Custodians returning excess material to the MCMO.

STEP 1. Verify the Custodian's ID Card against the command's "Authorization to Receipt" letter.

STEP 2. The Unit Custodian brings an "Account-Account Transfer" SF-153 with returned material as reflected per reference (a).

STEP 3. The D&A Chief and Unit Custodian will place the material on the working counter and verify material against the SF-153 and CSPM-3/Effective Status messages. The MCMO will not accept superseded material.

STEP 4. The D&A Chief will update the Unit Allowance Card, initial the SF-153 and pass the SF-153 to the Vault Operations Chief for processing per reference (a).

MCMO IOP

CHAPTER 5

DISTRIBUTION PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
GENERAL.....	5000	5-3
EXERCISE DISTRIBUTION PROCEDURES.....	5001	5-3
PULLING TEAM PROCEDURES.....	5002	5-3
DOUBLE CHECK TEAM PROCEDURES.....	5003	5-4
FINAL CHECK TEAM PROCEDURES.....	5004	5-4
DISTRIBUTION PROCEDURES.....	5005	5-4

MCMO IOP

CHAPTER 5

DISTRIBUTION PROCEDURES

5000. GENERAL. The MCMO provides distribution for exercises and contingency operations that require CINCPAC, CENTCOM, or Intertheater COMSEC Package keying material. Units deploying to major exercises will receive effective editions and one month Reserve On Board (ROB). The 31st MEU and units deploying for contingency purposes will receive effective editions and three months ROB. Follow-on distribution for contingency operations will be via DCS shipment, Over-the-Air Transfer (OTAT) or forward deployed MCMO.

5001. EXERCISE DISTRIBUTION PROCEDURES. Upon publication of an exercise "COMSEC CALL-OUT", units will determine material requirements/date materials required and send appropriate message to the MCMO as outlined in reference (c). The D&A Chief will take the request for action, review the Unit Allowance Card and confirm requirements via phone conversation with the unit CMS Custodian. The D&A Chief will submit the materials required via "Skinny Sheet" to the Vault Operations Chief who will prepare the "Transfer" SF-153 and retrieve material for transfer/pick-up. The Pulling, Double Check and Packing Teams require six different individuals (to include three different Custodians) to verify that material to be issued is accurate.

5002. PULLING TEAM PROCEDURES

STEP 1. The Vault Operations Chief (Reader) and a MCMO Custodian/CMS Clerk (Puller) will retrieve material appearing on each SF-153. The "Reader" will call out the short title, edition, quantity and accounting numbers for the "Puller" to retrieve.

NOTE: This constitutes the first security check on material being pulled, both "Reader" and "Puller" will exercise extreme caution and close attention to detail when pulling the material. The "Reader" will pronounce each word and number distinctly to ensure the correct material is removed from the shelves.

STEP 2. The "Puller" will remove the material from the shelf, read back the short title, edition, quantity and accounting numbers for the "Reader" to verify against the SF-153.

STEP 3. The material pulled will be placed on the working counter in the same order as reflected on the SF-153.

STEP 4. The Reader and Puller will initial on the bottom left corner of the SF-153 and attached "Skinny Sheet."

5003. DOUBLE CHECK TEAM PROCEDURES

STEP 1. The D&A Chief/Custodian (Reader) will read the short titles, editions, quantities and accounting numbers from the SF-153 while another MCMO Custodian/CMS Clerk (Verifier) sights the material on the working counter. Discrepancies will be reported to the Vault Operations Chief.

STEP 2. Once the "Double Check Team" is certain that the material is correct they will place their initials on the bottom right of the SF-153 and on the attached "Skinny Sheet."

5004. FINAL CHECK TEAM PROCEDURES

STEP 1. The "Reader" Administrative Chief/Custodian will select a box to accommodate the material and read aloud all short titles, editions, quantities and accounting numbers on the material on the SF-153, while the "Packer" places the called-out material in the box.

STEP 2. If the shipment/issue requires more than one box, the "Reader" will annotate the total number of boxes in the "REMARKS" column of the SF-153 and the "Skinny Sheet." Ex. 1/4, 2/4, 3/4

STEP 3. After the material has been verified the "Reader" and "Packer" will initial at the top of the SF-153 and on the "Skinny Sheet." The box is then secured and forwarded to the D&A Chief for issue.

5005. DISTRIBUTION PROCEDURES

STEP 1. Once the Unit Custodian and TPI designated individuals arrive for pick-up, the D&A Chief will verify the Unit Custodian's ID Card against the command's Authorization Message. If any

identification information is incorrect (i.e., SSN has inverted numbers, name is misspelled, etc.) the material will not be issued. There are no exception to this policy.

STEP 3. The D&A Chief will supervise the Unit Custodian and TPI designated individual during the inventory of material. The Unit Custodian will sign the SF-153 and initial the "Skinny Sheet" when he/she is satisfied that the material requested is present and reflected on the SF-153.

STEP 4. The D&A Chief will ensure the Unit Custodian accurately signs and dates the SF-153 and returns a copy to the Unit Custodian and the original to the Vault Operations Chief. The D&A Chief will maintain the "Skinny Sheet."

MCMO IOP

CHAPTER 6

PROCEDURES FOR PREPARING CMS MATERIAL FOR SHIPMENTS

	<u>PARAGRAPH</u>	<u>PAGE</u>
PREPARING SHIPMENTS.....	6000	6-3
SHIPMENTS/TRANSMITTALS.....	6001	6-3

MCMO IOP

CHAPTER 6

PROCEDURES FOR PREPARING CMS MATERIAL SHIPMENTS

6000. PREPARING SHIPMENTS

STEP 1. The "Wrapper" will seal the inner and outer seams of the box with brown tape, pack the box tightly and ensure all material is cushioned.

STEP 2. Place the original and Copy #2 of the SF-153 into the box.

STEP 3. Return Copy #3 of the SF-153 to the Vault Operations Chief to be maintained until signed SF-153 is returned.

STEP 4. Stamp the inner box with the appropriate "classification" stamp twice on each side and place the SF-153 within the box. Ensure that only one box is marked "Receipts Enclosed" when sending multiple boxes to the same account.

STEP 5. Weigh the box and annotate on the outer label and "Skinny Sheet." Verify the DCS address and transaction number on the "Skinny Sheet" with the D&A Chief prior to annotating on the label. Place the label on the side of the box and cover with cellophane tape.

STEP 6. Once the box is completely wrapped and labeled, place it on the outgoing shelf and return the "Skinny Sheet" to the D&A Chief.

NOTE: If a shipment is being containerized, place the individual boxes in the container. Cover all open and exposed seams. After the container is sealed, band it with two metal bands. Place two outer labels on the side and one on the end of the container. Cover the entire label with cellophane tape. Record the total weight of all the inner boxes plus 15lbs on the container level. Containers will not exceed 300 lbs.

6001. SHIPMENTS/TRANSMITTALS

1. Methods of Shipping/Transmittal. COMSEC material must be shipped per procedures outlined in reference (a).

2. Courier Accompaniment. COMSEC material shipment must be under the control of appropriate couriers. See reference (a) for the policy governing courier appointment.

3. See the Classified Material Control Center (CMCC) Officer for shipments via U.S. Postal Service and Armed Forces Courier Service.

MCMO IOP

CHAPTER 7

CMS EMERGENCY ISSUE PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
EMERGENCY ISSUES.....	7000	7-3
PROCEDURES.....	7001	7-3

FIGURE

7-1	SAMPLE ALLOWANCE CARD.....	7-4
-----	----------------------------	-----

MCMO IOP

CHAPTER 7

CMS EMERGENCY ISSUE PROCEDURES

7000. EMERGENCY ISSUES. Emergency issue of CMS material will be over-the-counter issues; however, delivery via DCS is also possible. The COMSEC Management Officer and MCMO Chief will normally respond to emergency taskings and direct issuance of required material.

7001. PROCEDURES

STEP 1. The senior custodian obtains the Unit Allowance Card for the CINCPAC/CENTCOM Area of Responsibility (AOR) and "Authorized to Receipt" letter/message.

STEP 2. The junior custodian logs into the ANCRS and prepares an "Account to Account Transfer" SF-153 based on the Unit Allowance Card.

STEP 3. The Senior Custodian "Reader" calls-out the material required (short title/edition/quantity/accounting number) to the Junior Custodian "Puller" who reads it back and places it on the working counter in sequential order.

STEP 4. The Custodians will reverse their roles during the "Double Check/Packing." The shipment will be prepared and distributed per procedures outlined in chapter 6.

STEP 5. The supported unit will arrive with an "Account-to-Account Transfer Report" (to include a TN) and return all keying material not required. The MCMO will return a copy of the SF-153 to the supported unit and report the transaction to DCMS.

STEP 6. The MCMO will then issue material per chapter 4 of this Manual and secure the vault/safe.

MCMO IOP

USCINCPAC ACR

TYPE UNIT: INFANTRY BATTALION

AKAI-XXXX
ICP
CALLSIGNS

AKAC-XXXX
ICP
AUTHENTI

AKAI-XX
ICP
NUCODES

AKAV-XXXX
ICP
JCEOI

USKAT-XXXX
ANDVT

USKAT-XXXX
PARKHILL

USKAT-XXXX
VINSON

USKAT-XXXX
128-BIT GEN

USKAT X-XXXX
CINCPAC
FASCINATOR

USKAT X-XXXX
CINCPAC
COLD START

USKAK X-XXXX
CINCPAC
KL-43

AKAC-XXXX
CINCPAC
AUTHEN

USKAK A XXXX
CINCPAC
KL-43

USKAT-XXXX
CINCPAC
VINSON

USKAT-XXXX
CINCPAC
PARKHILL

USKAT X-XXXX
CINCPAC
ANDVT

MCMO IOP

CHAPTER 8

DESTRUCTION PROCEDURES

	<u>PARAGRAPH</u>	<u>PAGE</u>
DESTRUCTION PREPARATION.....	8000	8-3
DESTRUCTION PULL TEAM PROCEDURES.....	8001	8-3
DESTRUCTION DOUBLE CHECK TEAM PROCEDURES.....	8002	8-4
FINAL CHECK TEAM.....	8003	8-4
PHYSICAL DESTRUCTION TEAM.....	8004	8-4

MCMO IOP

CHAPTER 8

DESTRUCTION PROCEDURES

8000. DESTRUCTION PREPARATION. The Vault Operations Chief will prepare for destruction in the following manner.

STEP 1. Verify the accuracy of the CMS 2-1A/3/4 against the CSPM-3 and effective status messages.

STEP 2. Verify that the MCMO account maintains items listed on the CMS 2-1A/3/4. If material is missing, check the Transaction Log to determine if the material was issued or destroyed. If verified, write the TN/date next to the missing material and notify the MCMO Chief immediately.

STEP 3. Verify disposition codes to ensure material with "DAZ" status is not destroyed until the succeeding edition is received.

STEP 4. Check the stock shelves to verify that earlier editions have been superseded. Place previously superseded material in a separate "Add-On" and prepare the appropriate destruction report per reference (a).

STEP 5. Prepare appropriate destruction reports and submit to the MCMO Chief. The MCMO Chief will assign MCMO Custodians and CMS Clerks to either the Destruction Pull, Double Check or Final Check Teams and task them with performing the destruction. The Vault Operations Chief will supervise the destruction procedure.

8001. DESTRUCTION PULL TEAM PROCEDURES

STEP 1. The MCMO Custodian "Reader" will call out short titles and editions to the "Puller" who locates; pulls the material; reads back the short title/edition; verifies that there are no earlier editions on the shelves; and places the material on the working table.

STEP 2. If no discrepancies are found the "Reader" will indicate that the material was pulled by placing a slant (/) in pencil adjacent to the accountability code on the CMS 2-1A/3/4.

8002. DESTRUCTION DOUBLE CHECK TEAM PROCEDURES

STEP 1. The "Reader" will call out short titles, editions, accounting numbers and quantities from the material on the working table.

STEP 2. The "Checker" (MCMO Custodian) will ensure all material matches the CMS 2-1A/3/4.

STEP 3. If no discrepancies are found, the "Checker" will cross (X) the Pull Team's check (/). Place no marks other than those required on the CMS 2-1A/3/4.

8003. FINAL CHECK TEAM

STEP 1. The "Reader" will call-out the short titles, editions, accounting numbers and quantities of the material.

STEP 2. The "Final Checker" will place a black dot next to the beginning and ending accounting number on the CMS 2-1A/3/4.

8004. PHYSICAL DESTRUCTION TEAM. The Physical Destruction Team will destroy the material as prescribed in reference (a), sign the destruction document and return the SF-153 to the Vault Ops Chief.